结合深度置信网络和模糊集的虚假交易识别研究

张李义　刘　畅
(武汉大学信息管理学院　武汉 430072)

摘要: 【目的】解决电子商务平台中存在的虚假交易问题。【方法】依据消费者历史购买和评论行为数据，提出一种结合深度置信网络和模糊集的虚假交易识别方法，通过识别虚假交易的用户(刷客)进行虚假交易的识别。【结果】识别准确率达到89%，与浅层机器学习模型试验结果进行对比，其综合性能有明显提升。【局限】相对于淘宝存在的海量刷客，实验数据较少。仅以淘宝数据作为验证数据，未涉及其他电子商务平台。【结论】本方法能够较好地识别刷客，减少电子商务中的虚假交易问题。

关键词: 虚假交易　刷客识别　商品评论　深度学习　模糊集
分类号: G202

1 引　言

目前电子商务呈快速发展态势，交易金额不断扩大，据中国电子商务研究中心统计[1]，截至2014年底中国网络零售交易规模达2.82万亿元人民币，超过美国成为全球第一大网络零售市场。巨大的市场吸引着更多的人投入到电子商务市场中。据赛迪网统计[2]，截止到2013年底淘宝店铺数量达900万家，同时每天的在线商品数已经超过8亿件。庞大的商品数量和商家数量意味着激烈的竞争，为了使店铺和商品在搜索中排名靠前，吸引消费者浏览和购买，出现了依靠虚假交易提高店铺信誉值和提高商品销量的欺诈行为。在中国，以刷单为目的的虚假交易行为已经形成庞大的利益链，有专门提供刷单服务的公司为卖家提供刷单服务，为了增加商品销售量、提高商家以及商品的信誉度，刷客必须给卖家好评，而好评对于用户的购买决策会产生巨大影响，并且产品的评价数量也决定了用户在商品详情页停留的时间。消费者在淘宝进行购物时，也多以产品销量和产品评论为主要依据，进行商品的选择。但是虚假的销量和评论会对消费者的购买决策产生巨大的误导作用，严重损害消费者的利益。因此识别虚假交易和虚假评论对电子商务的健康发展具有重要的意义。

2 文献综述

虚假评论是虚假交易中的重要组成部分，虚假评论是指不以事实为依据，对商品给予正面积极的评论以促进该产品的销售，或者给予商品负面消极的评论以破坏产品的名声。目前，对虚假评论的识别研究主要有两个方向：直接从评论本身出发识别虚假评论；通过识别虚假评论发布者识别虚假评论。所采用的识别方法则主要是支持向量机(SVM)、K最近邻算法(KNN)、人工神经网络(ANN)等有监督学习算法，虽然可以达到不错的分类效果，但是需要大量的标记数据集进行训练，耗费了大量的人工成本。并且特征的选择同样会对识别结果产生影响。

在基于评论本身的虚假识别方面，Jindal等[3-4]将垃圾评论分为虚假评论、无关评论和非评论信息三种，并且通过检测意外规则和规则聚类提出识别可疑评论的方法。Ott等[5]采用标准词和词性N-gram特征对来自Amazon Mechanical Turk的虚假评论和来自Tripadvisor

通讯作者：刘畅，ORCID：0000-0002-6775-2587，E-mail：liuchang0310@163.com。

.com的非虚假评论进行监督学习，利用SVM对特征进行分类，从而识别出虚假评论。任亚峰等[6]认为虚假评论与真实评论在语言结构和情感极性上存在差异，提出基于遗传算法，对语言结构及情感极性特征进行优化选择，并利用选取的特征结合硬、软聚类算法对虚假评论进行识别。Feng等[7]使用基于概率的上下文无关句法文体学规则特征识别虚假评论，用SVM分类器进行真实与虚假文本分类，并在标准数据集上进行验证。

除了针对评论本身的研究外，也有学者根据评论者的评论行为特征进行虚假评论的识别，Fei等[8]通过研究评论的集中爆发鉴别虚假评论者。他们认为在同一爆发周期内出现的评论有相同的特性，这些评论或全由虚假评论者发布，或全由真实评论者发布，基于此推断评论者是否为虚假评论者。Lim等[9]通过评论者异常打分行为识别虚假评论者，若评论者对商品连续进行过高或过低的打分，其为虚假评论者的可能性越大。Jiang等[10]总结了垃圾评论者的两种行为模式：短时期内对某一商品进行持续评论和商品的实际购买量相对于用户对商品的好评严重不符。通过分析用户评价行为和对商品评价的偏差分析识别垃圾评论。

从以上总结中可知，前人主要从被评论的主体入手，对其所有评论信息进行分析，并未从评论者在某一平台的所有历史评论数据的角度入手，研究用户是否为虚假评论者。此外前人在进行虚假评论识别方面采用的是浅层机器学习模型，比如 SVM、KNN 等，这些模型为有监督学习模型，需要大量有标记样本进行学习，会耗费大量人工标记时间成本。浅层模型主要依靠人工经验抽取样本的特征，而模型主要是负责分类或预测，在运用模型不出差错的前提下，特征的好坏成为整个系统性能的瓶颈[11]。与传统的浅层学习不同，深度学习通过逐层特征变换，将样本在原空间的特征表示变换到一个新特征空间，从而使分类或预测更加容易，展现了强大的从少数样本集中学习数据集本质特征的能力[12]。对于深度学习的研究则多集中于语音识别[13]、自然语言处理[14]和图像处理[15]等领域。深度置信网络(DBN)是由若干层无监督的受限玻兹曼机(RBM)和一层有监督的反向传播网络(BP)组成的一种深层神经网络，是深度学习中的一种机器学习模型[16]。相对于较早出现的有监督深度学习模型——卷积神经网络(CNNs)以及传统的有监督浅层学习模型，DBN 作为半监督深度学习模型，可以采用大规模无标签的样本集合，为 DBN 训练提供大量的样本，省去了标注大量样本的时间，并且其无监督学习过程能够学习到更准确的特征，克服了局部最优的局限。其次 DBN 作为深层网络学习结构，能够学习抽象特征，弱化浅层结构的错误特征，从而提高模型分类效果和缓解过拟合现象。另外，同样作为深度学习模型的卷积神经网络[17]是为识别二维图像而特殊设计的一个多层感知器，在图像处理方面具有众多优势，却不适合本文场景。

深度学习模拟人脑的机制解释数据，其分层理论就是基于神经科学，较低的层次学习和处理较初级的输入，其结果会送入较高的层次，较高的层次进而学习较高级的特征。在 Zeki [18]的研究中，知识来源于先天继承或者后天获取，先天继承的知识是不可变的，但是获取知识的先兆和预先对事物的假设会对人类有用，后天获取的知识可以通过经验以及内在无意识的思考方式进行进一步的修正。以上即采用模糊集理论模拟继承知识，采用 DBN 模拟后天获取的知识的动机。模糊集是描述和处理具有不确定性事物和现象的一种数学手段，将人们认识事物从传统的二值逻辑转换为[0,1]区间上的逻辑，可以广泛应用于模式识别中[19]。在模式识别中采用模糊集理论，可以描述事物属于一个类别或其他类别的程度[20]。在进行刷客识别的过程中，将用户“是刷客”或者“不是刷客”的逻辑转换为隶属度，在深度学习中引入模糊集概念，可以有效提高预测的准确度。其中 Fu 等[21]在中文语句级语义分类中引入了模糊集理论，采用直接方法模型化情绪极性分类的内在模糊性。笔者利用 DBN 和模糊集，提出一种结合深度置信网络和模糊集的虚假交易识别方法，并与浅层机器学习模型 KNN 和 SVM 进行性能对比。

3　特征提取

为了进行刷客的识别，笔者从淘宝评论数据中分别识别出刷客和正常用户，并利用其三个月的评论和购买数据进行特征提取。在淘宝网中，对卖家和买家有着相似的信用评价指标，分别是商家信用积分和买家信用积分。这只是描述买家和卖家的两个简单的评价标准，并不能准确分辨出正常买家和刷客，因此需

要提取出其他衍生属性对用户的行为进行描述，以便准确定义真实用户和刷客。Whitrow等[22]指出不同的统计时间周期会对统计模型产生关键的影响，过短的时间周期会导致不能捕获到足够的消费者的消费和评论历史，太长的时间周期又会产生过多的干扰噪声并且可能隐藏某些可识别的相关特征。因此适当的统计时间周期将会对刷客的识别产生重要的影响。

(1) F1：注册时间

注册时间短的用户更有可能成为刷客。由于刷客本身也是消费者，也会在淘宝进行消费活动，为了防止由于刷单被惩罚，往往会额外注册一个账号进行刷单活动，即使由于刷单行为被惩罚也不会影响自己的正常消费，降低了惩罚的成本。以用户注册时间至收集到的用户最后一条评论的时间距离作为用户的特征度量。

(2) F2：实名认证状态

未实名认证的用户更有可能成为刷客。实名认证可以更好地保障用户的资金安全，可以更方便地进行消费活动以及出现质量和服务争端时保障自己的利益，因此正常消费者大多会进行实名认证。刷客并不以消费为目的，为了保护自己的个人信息，往往不会进行实名认证，即使在被发现虚假交易行为时，匿名状态也可以很好地隐藏自己。以0代表用户未进行实名认证，1代表用户已进行实名认证作为用户的特征度量。

(3) F3：商品类别总数

购买商品类别越多的用户，越有可能是刷客。刷客会为了客户的需求，购买客户所要求的商品，并不以自己的真实购买意愿影响购买行为，因此在一定时期内其购买的商品类别会高于正常的用户。以收集到的最后一条评论的时间为节点，统计用户的购买商品类别总数作为用户的特征度量。

(4) F4：单日购买商品类别数

以收集到的最后一条评论的时间为节点，统计用户过去一个月平均每个购买日购买商品类别的数目作为用户的特征度量。

(5) F5：评论长度

评论字数差异较大的人都有可能是刷客。以评论者所有评论字数之和与评论总数的比值作为用户的特征度量。

(6) F6：单日评论数

平均每天评论较多的人更有可能是刷客。为了协助商家欺骗消费者并且使虚假交易显得更加真实，刷客每完成一笔虚假交易，都会对商品进行评论，因此在一定时期内，刷客平均每天的评论数会高于普通用户。以收集到的最后一条评论的时间为节点，统计用户过去一个月平均每个购买日评论商品的数目作为用户的特征度量。

(7) F7：单月评论数

以收集到的最后一条评论的时间为节点，统计用户过去三个月平均每月评论商品的数目作为用户的特征度量。

(8) F8：重复评论率

重复评论率越高的人越有可能是刷客。刷客以完成的虚假交易数量为获取利益的标准，并且在对商品进行评论时采用的是刷单中介提供的评论内容，因此刷客的重复评论率要高于普通用户。以收集到的最后一条评论的时间为节点，统计重复评论数与评论总数的比值作为用户的特征度量。

(9) F9：有内容评论率

有内容评论率越高的人越有可能是刷客。评论是刷客在进行虚假交易过程中的一个必须的步骤，因此刷客的有内容评论率往往要高于普通用户。以收集到的最后一条评论的时间为节点，统计评论者评论总数与评论者信用积分的比值作为用户的特征度量(其中评论者评论不包括匿名评论和系统默认好评)。

(10) F10：重复商家率

经常从同一商家购买商品的用户更有可能是刷客。新商家为了达到增加店铺信誉值的目的，会雇佣刷客多次进行虚假交易，因此刷客的购买记录中就出现商家重复率高的情形。以收集到的最后一条评论的时间为节点，统计重复商家数与购买商家总数的比值作为用户的特征度量。

(11) F11：消费者信用积分日增长率

信用积分增长快的用户更有可能是刷客。买家信用积分累积是针对订单中的每一项商品的，即订单交易成功后，卖家可以针对其中的每一项商品给买家做出评价，不同的评价会对消费者的信用积分有不同额度的增加。刷客以刷单作为盈利方式，为了获取更多的利益会进行较多的虚假交易，其信用积分增长速度

会高于正常的消费者。以平均每日消费者信用积分作为用户的特征度量，其值等于消费者信用积分/注册天数。

(12) F12：消费者信用积分月增长率

以平均每月消费者信用积分作为用户的特征度量，其值等于消费者信用积分/购买总月数。

图1是对数据集的统计性描述，利用消费者的购买行为特征揭示虚假交易和正常交易行为的不同。以衍生特征"单日评论数"为例，其中虚假交易者的单日评论数均值为5.764382，远高于正常交易者单日评论数均值2.350858，约为正常交易者的2.45倍。以此为例延伸至消费者购买的其他行为特征，均可发现其在数量上的明显不同。

图2是消费者行为特征独立样本T检验结果。其中"注册天数"方差方程Levene检验结果显示F值为0.009，Sig.值为0.925，表示方差齐性检验没有显著差异，故在均值方程的T检验结果中参照第一行数据，其中Sig.=.000，即两样本均数差别有显著性意义。其他行为特征的检验结果显示，显著性差异明显。

组统计量

	V1	N	均值	标准差	均值的标准误
注册天数	1	120	1091.75	689.417	68.942
	2	120	1836.48	705.447	70.545
实名认证状态	1	120	.48	.502	.050
	2	120	.93	.256	.026
商品类别总数	1	120	15.220000	1.5346503	.1534650
	2	120	11.038333	2.9425718	.2942572
单日购买商品类别数	1	120	.422290	.2676889	.0267689
	2	120	.800067	.1983297	.0198330
评论长度	1	120	21.832474	18.2857907	1.8285791
	2	120	20.447872	10.8240392	1.0824039
单日评论数	1	120	5.764382	4.7458898	.4745890
	2	120	2.350858	1.3349011	.1334901
单月评论数	1	120	3.067132	1.0319083	.1031908
	2	120	1.598257	.5560341	.0556034
重复评论率	1	120	65.341060	39.4144899	3.9414490
	2	120	11.254929	9.8180646	.9818065
有内容评论率	1	120	10.758702	2.8760318	.2876032
	2	120	4.311286	1.7474902	.1747490
重复商家率	1	120	.439862	.7802574	.0780257
	2	120	.119499	.1196288	.0119629
消费者信用积分日增长率	1	120	1.988489	1.9271292	.1927129
	2	120	.523005	.5619758	.0561976
消费者信用积分月增长率	1	120	264.000000	202.3434410	20.2343441
	2	120	147.661667	141.6899752	14.1689975

图 1　特征汇总统计结果

独立样本检验

		方差方程的 Levene 检验		均值方程的 t 检验						
									差分的 95% 置信区间	
		F	Sig.	t	df	Sig.(双侧)	均值差值	标准误差值	下限	上限
注册天数	假设方差相等	.009	.925	-7.550	198	.000	-744.730	98.638	-939.246	-550.214
	假设方差不相等			-7.550	197.895	.000	-744.730	98.638	-939.247	-550.213
实名认证状态	假设方差相等	277.666	.000	-7.981	198	.000	-.450	.056	-.561	-.339
	假设方差不相等			-7.981	147.353	.000	-.450	.056	-.561	-.339
商品类别总数	假设方差相等	52.837	.000	12.600	198	.000	4.1816667	.3318717	3.5272099	4.8361234
	假设方差不相等			12.600	149.146	.000	4.1816667	.3318717	3.5258891	4.8374442
单日购买商品类别数	假设方差相等	21.527	.000	-11.339	198	.000	-.3777772	.0333155	-.4434758	-.3120785
	假设方差不相等			-11.339	182.521	.000	-.3777772	.0333155	-.4435101	-.3120442
评论长度	假设方差相等	6.904	.009	.652	198	.515	1.3846025	2.1249234	-2.8057836	5.5749887
	假设方差不相等			.652	160.791	.516	1.3846025	2.1249234	-2.8117548	5.5809599
单日评论数	假设方差相等	7.575	.006	6.924	198	.000	3.4135243	.4930054	2.4413090	4.3857395
	假设方差不相等			6.924	114.567	.000	3.4135243	.4930054	2.4369363	4.3901123
单月评论数	假设方差相等	23.992	.000	12.531	198	.000	1.4688745	.1172181	1.2377184	1.7000307
	假设方差不相等			12.531	152.019	.000	1.4688745	.1172181	1.2372876	1.7004614
重复评论率	假设方差相等	98.296	.000	13.316	198	.000	54.0861310	4.0618917	46.0760095	62.0962524
	假设方差不相等			13.316	111.239	.000	54.0861310	4.0618917	46.0374117	62.1348502
有内容评论率	假设方差相等	42.466	.000	19.158	198	.000	6.4474167	.3365305	5.7837725	7.1110608
	假设方差不相等			19.158	163.330	.000	6.4474167	.3365305	5.7829052	7.1119281
重复商家率	假设方差相等	11.332	.001	4.058	198	.000	.3203622	.0789375	.1646961	.4760283
	假设方差不相等			4.058	103.652	.000	.3203622	.0789375	.1638200	.4769044
消费者信用积分日增长率	假设方差相等	45.824	.000	7.300	198	.000	1.4654837	.2007397	1.0696214	1.8613459
	假设方差不相等			7.300	115.717	.000	1.4654837	.2007397	1.0678831	1.8630843
消费者信用积分月增长率	假设方差相等	21.128	.000	4.710	198	.000	116.3383333	24.7020074	67.6255429	165.0511238
	假设方差不相等			4.710	177.269	.000	116.3383333	24.7020074	67.5904884	165.0861783

图 2　特征向量 T 检验结果

4　识别方法

深度置信网络(DBN)是目前研究和应用都比较广泛的深度学习结构，由一系列受限波尔兹曼机(RBM)单元组成。模糊集是描述和处理具有不确定性事物和现象的一种数学手段，在深度学习中引入模糊集概念，可以有效提高预测的准确度。

用 x^i 表示用户集 X 中的用户，用户集 X 则可以表示为：$X=[x^1,\cdots,x^{R+T}]$，其中 $x=[x_1,\cdots,x_D]'$，R 表示训练用户的数目，T 表示测试用户的数目，D 表示用户特

征的数目。用Y表示L个已经标记的训练集的标记，则可以表示为：$Y=[y^1,\cdots,y^L]$，其中 $y=[y_1,\cdots,y_c]'$，c 表示分类的数目。

深度置信网络训练的基本思想是一种半监督贪婪学习算法。模型训练过程主要分为两步：

(1) 分别单独地无监督训练每一层 RBM 网络。用未包含标注信息的训练数据训练第一层 RBM 网络，它由输入层 h^0 和第一层隐含层 h^1 组成，输入层接收的是原始的特征向量，训练时先学习输入层和第一层隐含层之间的参数 w^1。当训练好第一层 RBM 网络后，将第一层 RBM 网络的隐含层 h^1 作为第二层 RBM 网络的可视层，与第二层隐含层 h^2 组成第二层 RBM网络。第一层RBM网络的输出等于第二层RBM网络的输入，继续无监督地训练第二层 RBM 网络的参数 w^2。同理，在学习得到第 N−1 层 RBM 网络后，将第 N−1 层 RBM 网络的输出作为第 N 层 RBM 网络的输入，训练第 N 层 RBM 网络的参数 w^N，由此可以初始化 DBN 网络中各隐含层之间的参数空间 $W=[w^1,\cdots,w^N]$。

(2) 当完成逐层训练学习后，利用 BP 网络对整个 DBN 网络进行有监督反馈微调，根据输入特征向量和顶层降维表示传递之后的重构特征向量之间的误差，对整个网络权值进行微调。即将错误信息反向传递至所有 RBM 网络，微调 RBM 网络层间的参数。最后的结果即是 DBN 网络的最优参数[12,23]。

对于刷客识别，采用模糊集描述用户“是刷客”或者“不是刷客”的隶属度，其中模糊集 A 和 B 可以由以下进行描述[24]：

用 X 表示用户集，则 X 中的元素 x 表示用户集中的单个用户，X 中的正向模糊集 A 可以通过隶属度函数 $\mu_A(x)$ 进行表示，其中 $\mu_A(x)\in[0,1]$，表示 A 中 x 属于刷客的程度。负向模糊集 B 可以通过隶属度函数 $\mu_B(x)$ 进行表示，其中 $\mu_B(x)\in[0,1]$，表示 B 中 x 不属于刷客的程度。两个隶属度函数 $\mu_A(x)$ 和 $\mu_B(x)$ 都是通过深度结构第 N 层的结果 $h^N(x)$ 进行计算。

关于刷客的最终识别，只有两个类，即“是刷客”或“不是刷客”，所以深度学习第 N 层 $h^N(x)$ 的维度应该是 2，类分界线为 $h_1^N=h_2^N$。$h^N(x^i)$ 与分界线之间的距离可以表示为 $d(x^i)=(h_1^N(x^i)-h_2^N(x^i))/\sqrt{2}$，如果 $d(x^i)>0$，x^i 就是刷客，否则 x^i 就不是刷客。

隶属度函数 $\mu_A(x)$ 和 $\mu_B(x)$ 同距离 $d(x)$ 的关系可以用以下公式[25]表示：

$$\mu_A(x;\beta,\gamma)=\begin{cases}S(d(x);\gamma-\beta,\gamma-\beta/2,\gamma) & d(x)\leqslant\gamma\\ 1 & d(x)\geqslant\gamma\end{cases} \tag{1}$$

$$\mu_B(x;\beta,-\gamma)=\begin{cases}1 & d(x)\leqslant\gamma\\ 1-S(d(x);\gamma,\gamma+\beta/2,\gamma+\beta) & d(x)\geqslant\gamma\end{cases} \tag{2}$$

在识别过程中，需要估计两个参数β和γ的值，在图 3 中β=2，γ=1。由图 3 可知，γ是 $\mu_A(x)<1$ 和 $\mu_A(x)=1$ 的分界点(−γ是 $\mu_B(x)=1$ 和 $\mu_B(x)<1$ 的分界点)。β是 $\mu_A(x)$ 从 0 变化到 1 的距离 d(x)，同时也是 $\mu_B(x)$ 从 0 变化到 1 的距离。因此可以统计所有用户 x 的距离 d(x)的值来估计β和γ的值。对于基于 DBN 的刷客识别可以由以下公式描述：

$$\gamma=\max|d(x^i)|, i=1,\cdots,R+T \tag{3}$$

$$\beta=\xi\times\gamma, \xi\geqslant 2 \tag{4}$$

其中，ξ表示“是刷客”或“不是刷客”分界度的常数，可以根据不同的数据做具体的调节。

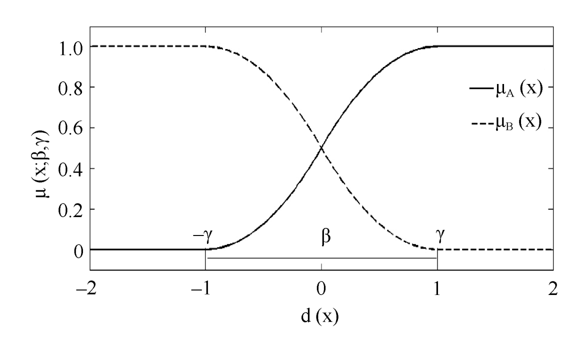


图 3　隶属度函数 $\mu_A(x)$ 和 $\mu_B(x)$

依据公式(3)和公式(4)估计模糊参数，建立深度结构。利用 L 个已经标记的数据和隶属度函数 $\mu_A(x)$ 和 $\mu_B(x)$ 再次优化参数空间 W 以提升判别的准确度，图 4 是采用模糊集概念的第 N–1 层的描述，以隶属度函数 $\mu_A(x)$ 和 $\mu_B(x)$ 作为输入函数。

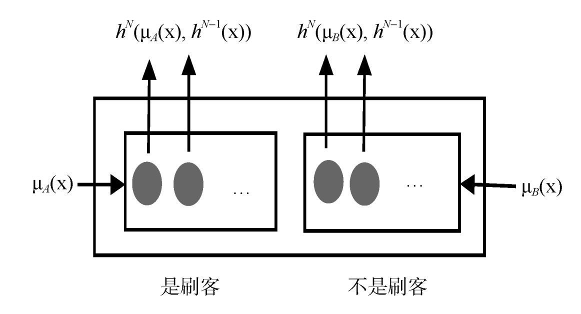


图 4　模糊层 h^{N-1} 层的描述

5　实验及结果分析

为了验证本文提出的识别方法的性能，从淘宝平台收集用户的购买数据，包括用户的性别、注册天数、信用积分、实名认证状态、购买商品名称、评论内容、用户对商品评分和评论时间。其中在收集数据过程中，为了满足训练集的要求，需要收集已经确定的刷客的数据。由于电子商务的发展，刷单已经成为一条庞大的利益链，其中比较大型的中介平台包括双赢网、百利网、刷客网等，它们通过发布商家订单信息和任务要求获取利润。为了获取真实的刷客信息，笔者根据以上平台发布的订单信息进入参与刷单的店铺，根据刷单的任务要求从商品评论信息中找到刷单用户。收集到用户信息之后，通过淘宝查询网站——淘大客对用户的基本信息和历史评论信息进行收集。对于正常用户的数据收集，笔者选择天猫店铺中信誉度高、影响力大，不需要通过刷单提高影响力的店铺(比如耐克官方旗舰店、小米官方旗舰店等)，从店铺的热销商品的评论页面中选取未匿名评论用户，从淘大客中搜索该用户的历史评论信息，如果该用户评论信息正常，比如评论内容客观、重复评论少并且未出现短期内大量评论的行为，即可判定此用户为正常用户。

在模糊集中，参数ξ表示“是刷客”或“不是刷客”的分界度，不同的值会影响准确率，为了找到最优的ξ，分别使用不同的值对数据进行测试，其测试结果如图 5 所示：

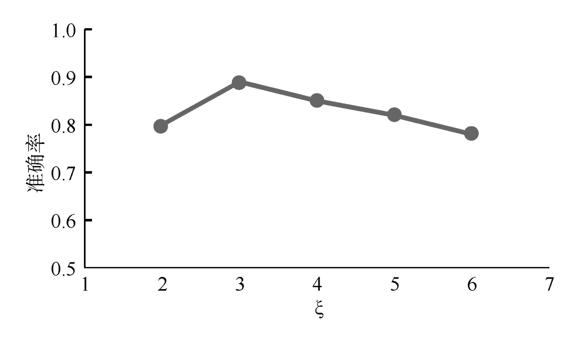


图 5　ξ值对准确率的影响

从图 5 中可以清楚地看出，当ξ=3 时识别准确率最高为 89%，因此在本文选取ξ=3。

图 6 中数字 1 表示刷客，–1 表示正常用户。在实验中选取 100 个用户作为测试集，其中重合的点表示正确识别的用户，未重合的点表示识别有误的用户。其中第一行未重合的实心点表示将正常用户误识别为刷客，第二行未重合的实心点表示将刷客误识别为正常用户。

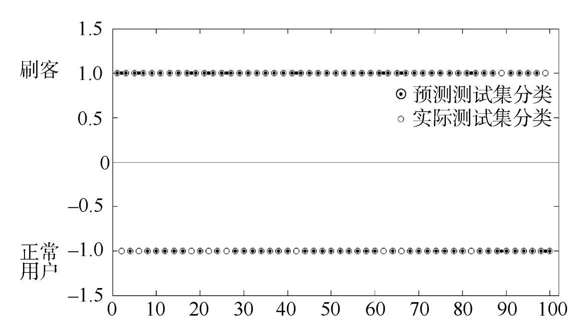


图 6　测试集的实际分类和预测分类对比

从图 6 中可以看出其中有 11 个用户识别错误，其准确率达到 89%。本文采用分类器中最常用的评测指标：准确率(Accuracy)、精确率(Precision)、召回率(Recall)作为刷客识别的评判标准，在进行评价的过程中将精确率和召回率结合在一起，使用 F-score 进行性能的评价[26]：

$$\text{Accuracy}=\frac{|TP|+|TN|}{|TP|+|FP|+|TN|+|FN|}$$

$$\text{Precision}=\frac{|TP|}{|TP|+|FP|}$$

$$\text{Recall}=\frac{|TP|}{|TP|+|FN|}$$

$$\text{F-score}=\frac{2\times\text{Precision}\times\text{Recall}}{\text{Precision}+\text{Recall}}$$

其中，|TP|表示把刷客正确地识别为刷客的数量；|FP|表示把正常用户错误地识别为刷客的数量。|TN|表示把正常用户正确地识别为正常用户的数量；|FN|表示把刷客错误地识别为正常用户的数量。

其分析结果如表1所示。与另外两种常用方法 KNN 和 SVM 相比，其精确率略低，但是 F-score 明显高于两者，其性能有明显提高。

表 1　DBN 和 SVM、KNN 分类方法的性能对比

方法	Accuracy	刷客		
		Precision	Recall	F-score
DBN	89%	84.21%	96%	89.72%
KNN	78%	85%	68%	75.56%
SVM	84%	85.42%	82%	83.68%

本文提出的方法结合深度结构的特征提取和模糊

集的模糊分类思想，在训练深度结构的过程中使用指数损失函数最大化类别的分离性。其次，采用同样的深度结构进行模糊参数的估计和刷客的分类，可以很好地提高这两个过程的一致性并且提高刷客识别的性能。因此模糊集和深度置信网络的结合提高了深度结构的识别能力。

6 结　语

本文提出结合深度置信网络和模糊集的虚假交易识别方法，主要根据虚假交易者(刷客)的行为特征，从海量用户中将其识别出来，认定其进行的交易为虚假交易。本文利用用户的历史评论和交易记录，提取可以表示用户行为的 12 个特征，并将其量化。其次根据深度置信网络和模糊集的概念，构建结合深度置信网络和模糊集的深度结构，针对用户是否为刷客设定一个模糊集，基于模糊信息对深度结构进行训练以提高识别能力。为了验证方法的可行性，从淘宝平台收集用户的历史评论和交易数据作为训练和测试集，对已经标记的用户数据进行训练学习，实验显示本文提出的方法其准确率、精确率、召回率、F-score 值分别达到 89%, 84.21%, 96%和 89.72%，识别效果明显优于已有的分类识别方法，对识别结果有明显的提升，达到了识别虚假交易的目的。

参考文献：

[1] 中国电子商务研究中心. 2014 年度中国电子商务市场数据监测报告[R/OL]. [2015-04-08]. http://www.100ec.cn/zt/upload_data/20150408.pdf. (China E-Business Research Center. The 2014 Report of China E-Business Market Data Monitoring [R/OL]. [2015-04-08]. http://www.100ec.cn/zt/upload_data/20150408.pdf.)

[2] "2014 年最成功电子商务网站"提名：淘宝网[EB/OL]. [2014-12-05]. http://miit.ccidnet.com/art/32559/20141205/5693755_1.html. (Taobao.com is Nominated for "The Most Successful Electronic Commerce Website in 2014" [EB/OL]. [2014-12-05]. http://miit.ccidnet.com/art/32559/20141205/5693755_1.html.)

[3] Jindal N, Liu B. Opinion Spam and Analysis [C]. In: Proceedings of the 2008 International Conference on Web Search and Web Data Mining (WSDM). 2008.

[4] Jindal N, Liu B, Lim E P. Finding Unusual Review Patterns Using Unexpected Rules [C]. In: Proceedings of the 19th ACM International Conference on Information and Knowledge Management (CIKM). 2010:1549-1552.

[5] Ott M, Choi Y, Cardie C, et al. Finding Deceptive Opinion Spam by Any Stretch of the Imagination [C]. In: Proceedings of the 49th Annual Meeting of the Association for Computational Linguistics: Human Language Technologies. 2011: 309-319.

[6] 任亚峰，尹兰，姬东鸿. 基于语言结构和情感极性的虚假评论识别[J]. 计算机科学与探索, 2014, 8(3): 313-320. (Ren Yafeng, Yin Lan, Ji Donghong. Deceptive Reviews Detection Based on Language Structure and Sentiment Polarity [J]. Journal of Frontiers of Computer Science & Technology, 2014, 8(3): 313-320.)

[7] Feng S, Banerjee R, Choi Y. Syntactic Stylometry for Deception Detection [C]. In: Proceedings of the 50th Annual Meeting of the Association for Computational Linguistics: Short Papers. 2012: 171-175.

[8] Fei G, Mukherjee A, Liu B, et al. Exploiting Burstiness in Reviews for Review Spammer Detection [C]. In: Proceedings of the 7th International AAAI Conference on Weblogs and Social Media. 2013, 13: 175-184.

[9] Lim E P, Nguyen V A, Jindal N, et al. Detecting Product Review Spammers Using Rating Behaviors [C]. In: Proceedings of the 19th ACM International Conference on Information and Knowledge Management. ACM, 2010: 939-948.

[10] Jiang B, Cao R H, Chen B. Detecting Product Review Spammers Using Activity Model [C]. In: Proceedings of the 2013 International Conference on Advanced Computer Science and Electronics Information (ICACSEI 2013). Atlantis Press, 2013:650-653.

[11] 余凯，贾磊，陈雨强，等. 深度学习的昨天，今天和明天[J]. 计算机研究与发展, 2015, 50(9): 1799-1804. (Yu Kai, Jia Lei, Chen Yuqiang, et al. Deep Learning: Yesterday, Today, and Tomorrow [J]. Journal of Computer Research and Development, 2015, 50(9): 1799-1804.)

[12] 孙志军，薛磊，许阳明，等. 深度学习研究综述[J]. 计算机应用研究, 2012, 29(8): 2806-2810. (Sun Zhijun, Xue Lei, Xu Yangming, et al. Overview of Deep Learning [J]. Application Research of Computers, 2012, 29(8): 2806-2810.)

[13] Dahl G E, Yu D, Deng L, et al. Context-Dependent Pre-trained Deep Neural Networks for Large-Vocabulary Speech Recognition [J]. IEEE Transactions on Audio, Speech, and Language Processing, 2012, 20(1): 30-42.

[14] Collobert R, Weston J. A Unified Architecture for Natural Language Processing: Deep Neural Networks with Multitask

Learning [C]. In: Proceedings of the 25th International Conference on Machine Learning. ACM, 2008: 160-167.

[15] Krizhevsky A, Sutskever I, Hinton G E. Imagenet Classification with Deep Convolutional Neural Networks [C]. In: Proceedings of the 26th Annual Conference on Neural Information Processing Systems. 2012: 1097-1105.

[16] Hinton G E, Osindero S, Teh Y W. A Fast Learning Algorithm for Deep Belief Nets [J]. Neural Computation, 2006, 18(7): 1527-1554.

[17] 李葆青. 基于卷积神经网络的模式分类器[J]. 大连大学学报, 2003, 24(2):19-23. (Li Baoqing. Building Pattern Classifiers with Convolutional Neural Networks [J]. Journal of Dalian University, 2003, 24(2): 19-23.)

[18] Zeki S. Splendors and Miseries of the Brain: Love, Creativity, and the Quest for Human Happiness [M]. The 2nd Edition. John Wiley & Sons, 2011.

[19] Mendel J M. On a Novel Way of Processing Data that Uses Fuzzy Sets for Later Use in Rule-based Regression and Pattern Classification [J]. International Journal of Fuzzy Logic and Intelligent Systems, 2014, 14(1): 1-7.

[20] Simpson P K. Fuzzy Min-Max Neural Networks. I. Classification [J]. IEEE Transactions on Neural Networks, 1992, 3(5): 776-786.

[21] Fu G, Wang X. Chinese Sentence-level Sentiment Classification Based on Fuzzy Sets [C]. In: Proceedings of the 23rd International Conference on Computational Linguistics: Posters. Association for Computational Linguistics, 2010: 312-319.

[22] Whitrow C, Hand D J, Juszczak P, et al. Transaction Aggregation as a Strategy for Credit Card Fraud Detection [J]. Data Mining and Knowledge Discovery, 2009, 18(1): 30-55.

[23] Leng B, Zhang X, Yao M, et al. A 3D Model Recognition Mechanism Based on Deep Boltzmann Machines [J]. Neurocomputing, 2015, 151: 593-602.

[24] Rutkowska P D. Neuro-fuzzy Architectures and Hybrid Learning [M]. Physica-Verlag HD, 2012.

[25] Zimmermann H J. Fuzzy Set Theory—And Its Applications [M]. Springer Netherlands, 2001.

[26] Wang X Y, Yang H Y, Li D M. A New Content-based Image Retrieval Technique Using Color and Texture Information [J]. Computers & Electrical Engineering, 2013, 39(3): 746-761.

作者贡献声明:

张李义: 提出研究思路, 设计研究方案;
刘畅: 进行实验, 采集、清洗和分析数据, 论文起草;
张李义, 刘畅: 论文最终版本修订。

收稿日期: 2015-06-26
收修改稿日期: 2015-10-14

Combine Deep Belief Networks and Fuzzy Set for Recognition of Fraud Transaction

Zhang Liyi　Liu Chang
(School of Information Management, Wuhan University, Wuhan 430072, China)

Abstract: [**Objective**] To solve the problem of fraud transaction in e-commerce platform. [**Methods**] This paper proposes a method that combine Deep Belief Networks and fuzzy set based on consumers' purchase history and reviews. Through recognizing the users in fraud transactions—cheaters to recognize the fraud transactions. [**Results**] Tested by experiments using the data crawled from Taobao.com, the accuracy can be achieved 89%. Compared with the shallow machine learning model, the comprehensive performance improves significantly. [**Limitations**] In contrast with the huge normal users and the users in fraud transactions, the experimental data in the paper is relatively small. And the test data only from Taobao.com, lack of the data from the other e-commerce platform to be validated. [**Conclusions**] The users in fraud transactions can be identified by the method, and the fraud transaction in e-commerce can be reduced.

Keywords: Fraud transaction　Cheater recognition　Product reviews　Deep learning　Fuzzy set